FISMA Implementation Project

Protecting the Nation's Critical Information Infrastructure

An Overview

Computer Security Division
Information Technology Laboratory

Today's Climate

- Highly interactive environment of powerful computing devices and interconnected systems of systems across global networks
- Federal agencies routinely interact with industry, private citizens, state and local governments, and the governments of other nations
- The complexity of today's systems and networks presents great security challenges for both producers and consumers of information technology

The Global Threat

- Information security is not just a paperwork drill…there are dangerous adversaries out there capable of launching serious attacks on our information systems that can result in severe or catastrophic damage to the nation's critical information infrastructure and ultimately threaten our economic and national security…

The Advantage of the Offense

- Sophisticated attack tools now available over the Internet to anyone who wants them
- Powerful, affordable computing platforms to launch sophisticated attacks now available to the masses
- Little skill or sophistication required to initiate extremely harmful attacks

Key Security Challenges

- Adequately protecting enterprise information systems within constrained budgets
- Changing the current culture of:

  "Connect first…ask security questions later"
- Bringing standards to:
  - ✓ Information system security control selection and specification
  - ✓ Methods and procedures employed to assess the correctness and effectiveness of those controls

Legislative and Policy Drivers

- Public Law 107-347 (Title III)
  Federal Information Security Management Act of 2002
- Homeland Security Presidential Directive #7
  Critical Infrastructure Identification, Prioritization, and Protection
- OMB Circular A-130 (Appendix III)
  Security of Federal Automated Information Resources

FISMA Legislation

Overview

"Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"

-- Federal Information Security Management Act of 2002

National Policy

Office of Management and Budget Circular A-130, *Management of Federal Information Resources* requires federal agencies to:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Authorize system processing prior to operations and periodically, thereafter

FISMA Tasks for NIST

- Develop standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Develop guidelines recommending the types of information and information systems to be included in each category
- Develop minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category

FISMA Implementation Project

- Phase I: To develop standards and guidelines for:
  - Categorizing federal information and information systems
  - Selecting minimum security controls for federal information systems
  - Assessing the security controls in federal information systems

Phase II: To create a national network of accredited organizations capable of providing cost effective, quality security assessment services based on the NIST standards and guidelines

Categorization Standards

NIST FISMA Requirement #1

- Develop standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Publication status:
  - ✓ Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
  - ✓ Final Publication: December 2003
  - ✓ Signed by Secretary of Commerce: February 2004

Mapping Guidelines

NIST FISMA Requirement #2

- Develop guidelines recommending the types of information and information systems to be included in each category described in FIPS Publication 199
- Publication status:
  - ✓ NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"
  - ✓ Final Publication: June 2004

Minimum Security Requirements

NIST FISMA Requirement #3

- Develop minimum information security requirements (i.e., management, operational, and technical security controls) for information and information systems in each such category—
- Publication status:
  - ✓ Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information Systems"*
  - ✓ Final Publication: December 2005

* NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems" (Second public draft projected for August 2004),will provide interim guidance until completion and adoption of FIPS Publication 200.

Certification and Accreditation

Supporting FISMA Requirements

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls)
- Publication status:
  - ✓ NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"
  - ✓ Final Publication: May 2004

Security Control Assessment

Supporting FISMA Requirements

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls)
- Publication status:
  - ✓ NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems"
  - ✓ Initial Public Draft: Summer 2004

Information Security Programs

Question

How does the family of FISMA-related publications fit into an agency's information security program?

Information Security Programs

Answer

NIST publications in the FISMA-related series provide security standards and guidelines that support an enterprise-wide risk management process and are an integral part of an agency's overall information security program.

Risk Management

Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Security accreditation
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Cryptography
- ✓ Firewalls and network security mechanisms
- ✓ Intrusion detection systems
- ✓ Anti-viral software
- ✓ Smart cards

Adversaries attack the weakest link…where is yours?

Managing Agency Risk

- Key activities in managing agency-level risk—risk resulting from the operation of an information system:
  - ✓ **Categorize** the information system
  - ✓ **Select** set of minimum (baseline) security controls
  - ✓ **Refine** the security control set based on risk assessment
  - ✓ **Document** security controls in system security plan
  - ✓ **Implement** the security controls in the information system
  - ✓ **Assess** the security controls
  - ✓ **Determine** agency-level risk and risk acceptability
  - ✓ **Authorize** information system operation
  - ✓ **Monitor** security controls on a continuous basis

Risk Management Framework

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

SP 800-53 / FIPS 200

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

Security Control Documentation

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

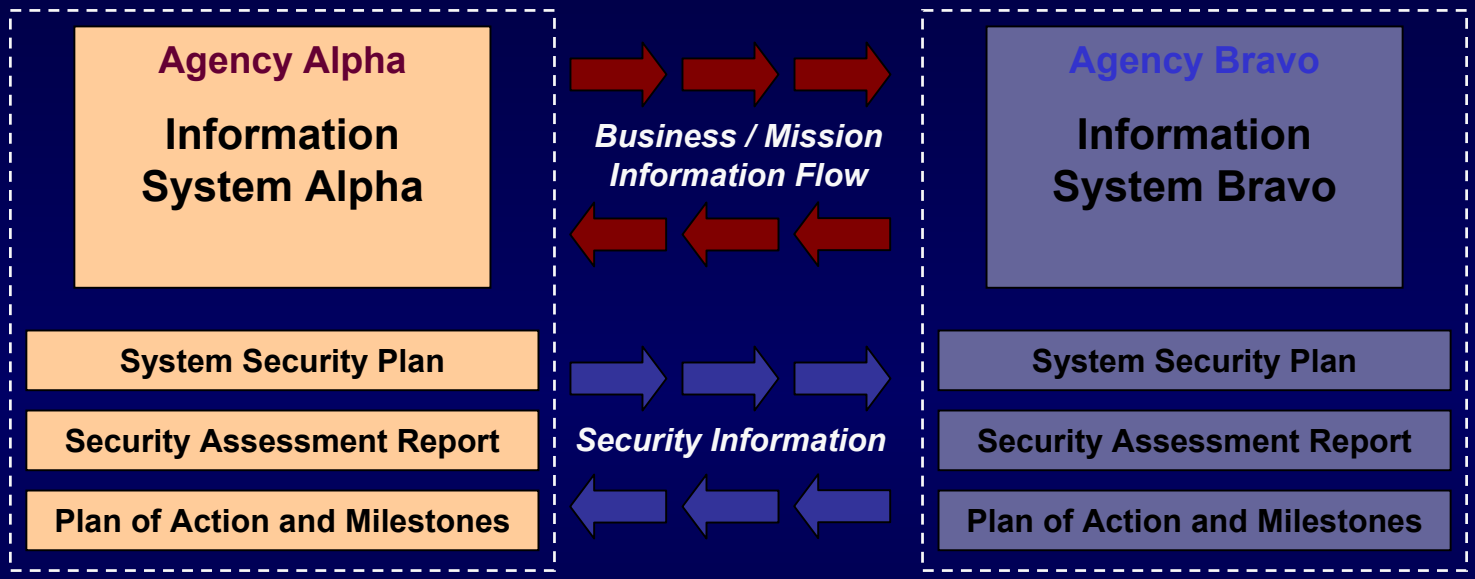
SP 800-53A / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

The Desired End State

Security Visibility Among Business/Mission Partners



Determination of risk to Agency Alpha's operations, agency assets, or individuals and acceptability of such risk

Determination of risk to Agency Bravo's operations, agency assets, or individuals and acceptability of such risk

The objective is to have *visibility* into prospective business/mission partners security programs BEFORE critical/sensitive communications begin…establishing levels of security due diligence.

FISMA Implementation Project

Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- NIST Special Publication 800-37 (C&A)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)
- FIPS Publication 200 (Minimum Security Controls)

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Manager

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Annabelle Lee
(301) 975-2941
annabelle.lee@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Gary Stoneburner
(301) 975-5394
gary.stoneburner@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Curt Barker
(301) 975-4768
wbarker@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov